🎯 Phishing Incident Response

🚨 1. Initial Detection & Triage

When to Trigger:

- A user reports a phishing email.
- Alert from email gateway (e.g., Microsoft Defender for Office 365).
- Suspicious login or abnormal behavior detected (e.g., Azure AD alert).

✅ 2. Immediate Actions (First 15–30 Minutes)

2.1 Acknowledge and Triage

- Acknowledge the user report.
- Log the incident in your IR tool (Jira, SIEM, or spreadsheet).
- Retrieve the full email (headers + body) from:
  - Defender for Office 365
  - Outlook Message Trace (via Exchange Admin Center or PowerShell)

2.2 Analyse the Email

- Inspect headers for spoofing or strange return paths.
- Detonate links or attachments in a sandbox (e.g., Joe Sandbox, Hybrid Analysis).
- Check reputation of links and attachments: VirusTotal, URLhaus, Defender Threat Intelligence

---

🔥 3. Containment (Windows-Specific)

3.1 If No Interaction (user didn't click/download):

- Add the sender to the blocklist in Microsoft Defender for Office 365.
- Search and remove the phishing email from other inboxes: Use **Microsoft PowerShell:**

```
#Get-MessageTrace -SenderAddress attacker@domain.com

#Search-Mailbox -Identity "username" -SearchQuery 'Subject:"phishing subject"' -DeleteContent
```

3.2 If Link Was Clicked (but no credentials entered):

- Check browser history/logs via:
    - BrowsingHistoryView
    - EDR tools like Defender for Endpoint or CrowdStrike
- Pull logs for potential DNS requests to the phishing domain: ipconfig /displaydns, Defender logs
- Block phishing domain at:
    - Endpoint firewall (Windows Defender Firewall)
    - Perimeter firewall / DNS filtering (e.g., Cisco Umbrella)

3.3 If Credentials Were Entered:

- Force password reset for the user via: Azure AD / Active Directory
- Revoke tokens and sessions:
- Enable MFA if not already active.
- Review sign-in logs for suspicious IPs and impossible travel

3.4 If Attachment Was Opened:

- Isolate the host using Defender for Endpoint:
    - Microsoft Defender Portal → Devices → Isolate Device
- Scan the machine:
  #Start-MpScan -ScanType FullScan
- Pull logs**:** Defender for Endpoint alerts, Windows Event Logs (Event Viewer) - Application Logs, Security Logs, Sysmon (if installed)
- Quarantine detected files manually or with:

  #Remove-MpThreat

🛠 4. Eradication

- Remove phishing email from all mailboxes.
- Remove any dropped payloads or registry persistence keys (check HKCU\Software\Microsoft\Windows\CurrentVersion\Run).
- Run: #Get-MpThreatDetection
- Clear temp directories (%TEMP%, %APPDATA%) if malware was involved.

🩺 5. Recovery

- Unisolate the machine after confirming it’s clean.
- Reset any impacted credentials or tokens.
- Inform the user of the incident and ensure they have received phishing awareness training.

📝 6. Reporting & Documentation

- Fill out post-incident report:
  - Timeline of events
  - Users affected
  - Tools/logs used
  - Actions taken
  - Root cause (malicious link, weak credentials, etc.)
- Save evidence (emails, logs, screenshots).

🔁 7. Lessons Learned / Review

- Conduct a brief internal review with:
  - IT
  - Security
  - Department where the user works
- Tune detections in:
  - Microsoft Defender policies
  - EDR rules
  - Email gateway filters
- Update playbook if gaps were identified.

🧪 8. Optional — Simulate & Train

- Use Microsoft Attack Simulator or GoPhish for simulated phishing campaigns.
- Train employees to report phishing via Outlook’s “Report” button or security inbox.

✅ Phishing Attack – Quick Checklist

- ✅ Identify suspicious emails or user reports
- ✅ Analyse email content, headers, and links
- ✅ Block malicious domains/URLs/IPs
- ✅ Isolate affected devices if a compromise is suspected
- ✅ Reset credentials for impacted accounts
- ✅ Check email logs for other recipients
- ✅ Scan endpoints for malware or unauthorized changes
- ✅ Remove phishing emails from all inboxes
- ✅ Report to security, HR/legal if needed
- ✅ Educate user(s) involved
- ✅ Update detection rules and awareness training
- ✅ Document and close the incident